



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/825,976	04/05/2001	Joonsang Baek	BAEK3001/EM/6671	3701

7590 10/19/2004
BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314-1176

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 10/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/825,976	Applicant(s) BAEK ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 April 2001.
 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1-5 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 05 April 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☒ None of:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2137

DETAILED ACTION

1. Claims 1-5 are pending.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Republic of Korea on 10/17/2000. It is noted, however, that applicant has not filed a certified copy of the 2000-60854 application as required by 35 U.S.C. 119(b).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fujisaki et al and further in view of Pointcheval.

As per claim 1, Fujisaki et al discloses a method for use in a public-key encryption system, the encryption system having

Art Unit: 2137

an encryption block encrypting a plaintext m a length k_0 output ciphertext (α, β) and a decryption block for decrypting the ciphertext (α, β) to provide the plaintext comprising the steps of: choosing variables p , q and g as public-key parameters, wherein p is large prime number of length q large prime number dividing $p-1$ and g a generator a multiplicative group Z_p^* wherein $Z_p^* = (g^0, g^1, g^2, \dots, g^{q-1})$; choosing publishing hash function H , $H: \{0,1\}^k \rightarrow Z_q$, providing security against adaptive-chosen-ciphertext-attack choosing and storing a secret key satisfying $x \in Z_q$ based chosen public-key parameters p , q and g and generating public X ($X=g^*$) thereby publishing the public-key parameters p , q and g and the public key encrypting plaintext m using the public key thereby generating the ciphertext (α, β) (see page 28 and page 31).

Fujisaki et al fails to disclose a second hash function G , $G: Z_p^* \rightarrow \{0,1\}^k$, providing security under computational Diffie-Hellman assumption; verifying whether the ciphertext (α, β) is valid and decrypting the ciphertext (α, β) verified be valid, ciphertext (α, β) by using the secret key x to recover the plaintext m .

However, Pointcheval teaches a second hash function and verifying whether the ciphertext (α, β) is valid and decrypting

Art Unit: 2137

the ciphertext (α, β) verified to be valid, ciphertext (α, β) by using the secret key x to recover the plaintext m (see page 7).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to apply Pointcheval's second hash function to Fujisaki et al's encryption scheme.

Motivation to do so would have been create a one-way encryption function that is secure against adaptively chosen-ciphertext attacks (see Pointcheval page 7).

As per claim 2, the modified Fujisaki et al and Pointcheval method discloses $(\alpha, \beta) = \{g^{H(m||r)}, G(X^{H(m||r)} \bmod p) \oplus (m||r)\}$ (see Fujisaki et al page 31 with the encryption box on Pointcheval page 7).

As per claim 3, the modified Fujisaki et al and Pointcheval method discloses computing $t = G(\alpha^x) \oplus \beta$ to determine if is α identical to $g^{H(t)}$ (see Pointcheval page 7).

As per claim 4, the modified Fujisaki et al and Pointcheval method discloses the decrypting step (f) includes the step of removing the random number r from t to thereby recover the plaintext m (see Pointcheval page 7 where it is inherent for the random bits to be removed to view the message).

As per claim 5, the modified Fujisaki et al and Pointcheval method discloses the exponentiation operation is replaced by

Art Unit: 2137

addition operation over elliptic curve group (see Pointcheval page 7).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Cramer et al discloses a public key system that is secure against adaptive chosen ciphertext attacks, Uchiyama et al discloses an encryption/decryption method which describes an adaptive chosen ciphertext attack, and Kiltz et al discloses secure public key encryption using random oracles.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP


Andrew Caldwell